WHAT IS CLAIMED IS:

Sub A1

1. A system for controlling Internet access on a network, said system comprising:

at least one access device for connecting to said network and for originating out-going data packets, each of said at least one access device being characterized by a unique hardware address;

a redirection server accessible via the Internet;

a network monitoring device for monitoring out-going data packets sent from said network to the Internet and for verifying if an originator access device of an out-going data packet is authorized for Internet access, all out-going packets originated from authorized access devices being forwarded unimpeded to the Internet and all out-going data packets originated from unauthorized access devices be being inspected for determination of their target destination Internet websites, and for checking if a determined target destination Internet website matches a predetermined authentication server website and forwarding a corresponding out-going data packet to said predetermined authentication server if a match is found, said network monitoring device responding to a match not being found by disregarding the determined destination Internet website and forwarding the out-going data packet to said redirection server;

whereby all out-going data packets to the Internet gain access to the Internet irrespective of whether their respective originator access devices are authorized for Internet access.

2. The system of claim 1 wherein said redirection server responds to a received data packet from an unauthorized originator access device by sending said originator access device a message instructing it to connect to said predetermined authentication server.

3. The system of claim 1 wherein said authentication server responds to an unsolicited received data packet by sending an originator access device of said data packet a questionnaire form soliciting authentication information, said questionnaire form including a hidden reserved field and a first identification keyword.

4. The system of claim 3 wherein said hidden reserved field is not accessible by said originator access device which receives said questionnaire form.

5. The system of claim 3 wherein said first identification keyword is based on address information from said network monitoring device.

6. The system of claim 3 wherein said network monitoring device, after verifying that said determined target destination Internet website matches said predetermined authentication server and before forwarding the out-going data to said predetermined authentication server, further scans contents of said out-going data packet in search of said first identification keyword and upon locating said first identification keyword, generates a second identification keyword based on the unique hardware

address of the originator access device, said second identification keyword being inserted in said hidden reserved field.

7. The system of claim 6 wherein said second identification keyword is additionally based on current communication session information.

8. The system of claim 6 wherein said second identification keyword is additionally based on location information of said network monitoring device.

9. The system of claim 6 wherein said hidden reserved field is located within said out-going data packet a predetermined number of bytes away from said first identification keyword.

10. The system of claim 6 wherein said hidden reserved field is immediately preceded by said first identification keyword within said out-going data packet.

11. The system of claim 3 wherein said originator access device receiving said questionnaire form uses web browsing software to supply said solicited authentication information into said questionnaire form before transmitting the questionnaire form back to said authentication server via the Internet.

12. The system of claim 1 wherein said authentication server responds to a solicited data packet having a hidden reserved field by extracting the contents of said hidden reserved field and authentication information from said solicited data packet, the extracted information being sent to a gate keeper server.

13. The system of claim 12 wherein said gate keeper server is accessible via the Internet.

14. The system of claim 12 wherein said authentication server uses a CGI script to parse said extracted information from said solicited data packet.

15. The system of claim 12 wherein said gate keeper server compares said authentication information with a predefined database to determine if said originator access device is registered, and responds to the verification of the originator access device being registered by sending an unblock message to said network monitoring device.

16. The system of claim 15 wherein said unblock message is encrypted with said second identification keyword.

17. The system of claim 15 wherein upon verification of the originator access device being registered, said gate keeper server decodes contents of said hidden

reserved field to determine the unique hardware address of said originator access device and labeling said unblock message with said hardware address.

18. The system of claim 15 wherein said network monitoring device responds to receipt of said unblock message by updating a network access list to authorize said originator access device for Internet access.

19. A system for remotely authenticating a user on a private network via the Internet, the system comprising:

a network access device for permitting said user access to said private network, said access device being characterized by a unique hardware;

an authentication server accessible via the Internet;

a network monitoring device for monitoring the destination address of all out-going messages from said private network to the Internet and for scanning the content of any message whose destination is said authentication server to search for a first predetermined identification code in said message, said network monitoring device responding to the detection of said first predetermined identification code by determining the hardware address of the access device that originated the message and generating a second identification code based on said hardware address, said network monitoring device further inserting said second identification code in said message before forwarding said message to said authentication server;

said authentication server responding to receipt of said forwarded message from said network monitoring device by decoding said hardware address from said

second identification code; a third identification code based on said hardware address being generated and transmitted along with an unblock message to said network monitoring device.

20. The system of claim 19 wherein said network monitoring device responds to said unblock message by updating a network access list to authorize for Internet access the user whose network access device has the same hardware address as is embedded in said third identification code.

21. The system of claim 19 wherein said second identification code is further based on the Internet protocol address of said network monitoring device.

22. The system of claim 19 wherein said third identification code is further based on the Internet protocol address of said network monitoring device.

23. The system of claim 19 wherein said network monitoring device responds to the absence of said first predetermined identification code in a message whose destination is said authentication server by forwarding said message to said authentication server with no modification to said message.

24. The system of claim 19 wherein said network monitoring device is further effective for verifying if an out-going message is originated by an authorized user and permitting all out-going messages from authorized users unimpeded access to the

Internet, all messages from unauthorized users having their destination addresses inspected to determined if their destination is said authentication server, and responding to a destination address other than said authentication server by ignoring the destination address and forwarding the message to a predetermined redirection server via the Internet;

whereby all out-going messages to the Internet are granted access to the Internet irrespective of whether the message is originated by an unauthorized user.

25. The system of claim 24 wherein said redirection server responds to a received message from an unauthorized user by sending the user's network access device a message instructing it to connect to said authentication server.

26. The system of claim 19 wherein said authentication server responds to a received message lacking said second identification code by generating said first predetermined identification code based on location information of said private network, said authentication server further sending the network access device that originated the message a questionnaire form soliciting authentication information from its respective user, said questionnaire form including a hidden reserved field and said first predetermined identification code.

27. The system of claim 26 wherein said hidden reserved field is not accessible by the user that receives said questionnaire form.

28. The system of claim 26 wherein said hidden reserved field is preceded by said first predetermined identification code in said questionnaire form.

29. The system of claim 26 wherein said network monitoring device inserts said second identification code in said hidden reserved field of any messages sent by a user to said authorization server.

30. The system of claim 26 further having a gate keeper server, said authentication server further being able to identified filled questionnaire forms received from unauthorized users and being effective for parsing out the user's authentication information along with said hardware address from said second identification code;

said authentication information and hardware address being relayed to said gate keeper server for verification, said gate keeper server responding to the verification of an unauthorized user by generating said third identification code and transmitting said unblock message to said network monitoring device.

31. The system of claim 30 wherein said gate keeper is accessed via a secure link from said authorization server.

32. The system of claim 30 wherein said authorization server accesses said gate keeper server via the Internet.